PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174796

(43)Date of publication of application : 23.06.2000

---

(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 9/32
H04L 12/66
H04L 12/56
H04L 29/14

---

(21)Application number : 10-347235 (71)Applicant : HITACHI LTD

(22)Date of filing : 07.12.1998 (72)Inventor : TSUCHIYA KAZUAKI
NOZAKI SHINJI

---

(54) MANAGEMENT METHOD FOR COMMUNICATION NETWORK SYSTEM, AND INFORMATION REPEATER

(57)Abstract:

PROBLEM TO BE SOLVED: To facilitate the prevention of eavesdropping and impersonation by a malicious user and the analysis and restoration of an address setting error.

SOLUTION: An LAN switch 11 constitutes the communication network of a virtual LAN(VLAN) 1 and the VLAN 2, etc., by arbitrarily connecting plural personal computers(PCs) 31-34 as network terminals to respective plural ports 21-25. In this

case, it is provided with a communication processing means 12 for transmitting and receiving packets with the respective ports 21-25, a relay processing means 13 for relaying the packets with the respective ports 21-25 based on a host table 14 updated by learning the change of the correspondence relation of the respective ports and the address information of the connected PC and an authentication processing means 15 for performing user authentication to the PC of a transmission origin by referring to an authentication table 16 and permitting the rewrite of the host table 14 and the relay of the packet only in the case of a true user at the time of the updating of the host table 14 of a packet relay trigger.

LEGAL STATUS [Date of request for examination] 01.08.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Two or more input/output port to which a network terminal or network repeating installation is connected, The control table which matches and stores either [at least] the network logical address given to each said input/output port and said network terminal, or network repeating installation or a network physical address, While delivering and receiving communication link information between said network terminal connected to each of two or more of said input/output port based on said control table, or network repeating installation By learning change of the correspondence relation between either [at least] said network logical address included in said communication link information or a network physical address and said input/output port, and updating said control table It is the management method of the communication network system using information repeating installation including the junction processing means which enables dynamic modification of said network terminal over said input/output port, or the connection condition of network repeating installation. Either [at least] said network logical address corresponding to each network terminal, or a network physical address. The 1st step which sets up the authentication table on which the user name and password of the network terminal concerned were stored by matching, When transfer of said communication link information accompanied by renewal of said control table occurs, in advance of transfer of said communication link information, and renewal of said control table, the transmitting origin of said communication link information and one [at least] user of a transmission place are received. User authentication which requires the input of said user name and a password, and collates it with said user name and password in the user name and password which were entered, and said authentication table is performed. The 2nd step which discards said communication link information while inhibiting renewal of said control table, when renewal of said control table and transfer of said communication link information are performed only when it succeeds in said user authentication, and said user authentication goes wrong, The management

method of the communication network system characterized by performing.
[Claim 2] In the management method of a communication network system according to claim 1 at said 1st step As opposed to either [at least] said network logical address or a network physical address One [at least] contact mail address of said user and the manager of a communication network system is also matched and set up. At said 2nd step While said user name inputted by said user of the transmitting origin of said communication link information or a transmission place in said user authentication is included The processing which sends out the message which notifies that the updating demand of said control table occurred to said user of said network logical address which creates and corresponds, or a network physical address, and one [at least] contact mail address of a manager, When said user authentication in said 2nd step goes wrong, while inhibiting renewal of said control table, said communication link information is discarded. When said user authentication in the separation of said input/output port which furthermore received the communication link information concerned and the processing which discards all the communication link information received from the input/output port concerned, and said 2nd step goes wrong, While inhibiting renewal of said control table, said communication link information is discarded. To the user of said all network terminals belonging to the still more nearly same virtual LAN (local area network) as said network logical address of the transmitting origin of this communication link information, or a network physical address The setting mistake of said network logical address or a network physical address, The processing which creates and sends the message which warns of the malicious user performing tapping and the communication link of spoofing using the address of other network terminals, The processing which performs said user authentication regardless of the existence of updating demand generating of said control table to the user of said network logical address registered into said control table periodically or irregularly, or a network physical address, ** -- the management method of the communication network system characterized by performing one processing even if few.
[Claim 3] Two or more input/output port to which a network terminal or network repeating installation is connected, The control table which matches and stores either [at least] the network logical address given to each said input/output port and said network terminal, or network repeating installation or a network physical address, While delivering and receiving communication link information between said network terminal connected to each of two or more of said input/output port based on said control table, or network repeating installation By learning change of the

correspondence relation between either [at least] said network logical address included in said communication link information or a network physical address and said input/output port, and updating said control table It is information repeating installation including the junction processing means which enables dynamic modification of said network terminal over said input/output port, or the connection condition of network repeating installation. Either [at least] said network logical address corresponding to each network terminal, or a network physical address. The user name of the network terminal concerned and a password, and the authentication table on which one [at least] contact mail address of said user and the manager of a communication network system was stored by matching, When transfer of said communication link information accompanied by renewal of said control table occurs, in advance of transfer of said communication link information, and renewal of said control table, the transmitting origin of said communication link information and said one [at least] user of a transmission place are received. While performing user authentication which requires the input of a user name and a password and collates it with said user name and password in the user name and password which were entered, and said authentication table While transmitting the message which notifies that said updating demand of the user name obtained by said user authentication to said one [at least] contact mail address of the transmitting origin of said communication link information and said manager and said control table occurred It is the information repeating installation characterized by having the control logic which performs actuation which discards said communication link information while inhibiting renewal of said control table, when renewal of said control table and transfer of said communication link information are performed only when it succeeds in said user authentication, and said user authentication goes wrong.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention is applied to the management method of the Internet work-piece equipment called a LAN (LAN: Local Area Network) switch (Layer2 a switch, Layer3 switch, etc.) and the communication network system (LAN switch network system) constituted from a LAN switch etc. about the management technique and information junction technique of a communication network system, and relates to an effective technique.

[0002]

[Description of the Prior Art] VLAN (VLAN: Virtual LAN) is in the description technique which a LAN switch has. VLAN is a technique which enables construction of LAN, without being dependent on the physical port of Internet work-piece equipment, and is known by the difference in the format under the name of the port base VLAN, the MAC (MAC: Media Access Control) address base VLAN, the Layer3 protocol base VLAN, IP (IP: Internet Protocol) subnet base VLAN, etc.

[0003] With the reference technique of this invention, if the packet from PC (PC: Personal Computer)231 to PC233 is received, the LAN switch 210 equipped with two or more ports 221-225 in the communication network system of IP subnet base VLAN shown, for example in drawing 7 will learn the starting point MAC Address of a packet, a terminal point MAC Address, and a starting point IP address, and will create a host table 220. Next, when an applicable entry is in a key with reference to a host table 220 about a terminal point IP address, a packet is outputted to an applicable port. When there is no applicable entry, it opts for the NeXT hop with reference to routing table (with no illustration), and an ARP (ARP: Address Resolution Protocol) table (with no illustration), and the entry of the corresponding host table 220 is created newly, and a packet is outputted to an applicable port. The LAN switch 210 is carried out in this way, and relays the packet to PC233 from PC231.

[0004] Furthermore, with the LAN switch 210, the entry of a host table 220 is discarded periodically, and since the entry of a host table 220 is always updated by newly learning from a packet, even when PC moves, a packet can be correctly relayed

to the port of a migration place. That is, PC can resume automatically the same communication link as migration before, even when it moves.

[0005]

[Problem(s) to be Solved by the Invention] However, there is the next technical technical problem in the above-mentioned reference technique.

[0006] The 1st technical technical problem is defenseless to the setting mistake of an IP address etc. For example, PC232 presupposes that the IP address of PC231 has been accidentally connected with a setup and a port 222. In this case, with the LAN switch 210, it will judge that PC231 moved to the port 222 from the port 221, and a host table 220 will be rewritten such. Consequently, the poor communication link of it becoming impossible to communicate etc. generates PC231 which is using the IP address correctly. Moreover, when there are many PCs connected to a network, analysis and recovery of this poor communication link take a great effort.

[0007] The 2nd technical technical problem is allowing tapping and spoofing by the malicious user. For example, suppose that PC235 connected the IP address of PC231 to the setup and the port 225. In this case, with the LAN switch 210, it will judge that PC231 moved to the port 225 from the port 221, and a host table 220 will be rewritten such. Consequently, the commo data addressed to PC231 will be able to be received and it will be able to intercept, and PC235 will turn into PC231, and will be able to clear up and communicate.

[0008] The purpose of this invention is to offer the management technique and information junction technique of the communication network system in which prevention of the poor communication link by the setting mistake of a logical or physical network address etc., and the cause analysis of a poor communication link and speeding up of recovery operation are possible.

[0009] Other purposes of this invention are to offer the management technique and information junction technique of the communication network system which can raise the security of a communication network system by preventing tapping and spoofing by the malicious user.

[0010]

[Means for Solving the Problem] This invention connects a user terminal and other repeating installation to two or more input/output port with which information repeating installation, such as a LAN switch, was equipped, and is built, and change of connection conditions, such as a user terminal to input/output port, is learned. By updating the control table which manages the correspondence relation between input/output port and a network address In the management method of the

communication network which can change dynamically the connection condition over the input/output port of each user terminal When the updating demand of a control table ignited by transfer of communication link information occurs between each user terminal (i.e., between two or more input/output port), Only when user authentication is performed to the user terminal of the transmitting origin of the communication link information concerned and it is checked that he is the user of Shinsei, the communication link information based on updating and it of a control table is made to deliver and receive.

[0011] Moreover, each user terminal and a system administrator's contact mail address are registered into some authentication tables on which the network address used for user authentication, a user name, a password, etc. were stored, and the message which described that the updating demand concerned occurred at the time of generating of an updating demand of a control table is sent to a user terminal, a system administrator, etc. of the transmitting origin of communication link information by e-mail. Under the present circumstances, regardless of the existence of a success of user authentication, the user name obtained in the user authentication concerned is stored in the message concerned.

[0012] More specifically, this invention has the following descriptions.

[0013] In the communication network system which constitutes this invention from the 1st viewpoint with a LAN switch It is the management method of the LAN switch network system which can prevent a poor communication link, and tapping and spoofing by the malicious user by the setting mistake of an IP address etc. For example, it sets to the communication network system of IP subnet base VLAN shown in drawing 1 . (a) Beforehand PCs 31-34 on the LAN switch 11 An IP address and its user name, Register a password and a contact mail address and the manager of the (b) LAN switch 11 registers a contact mail address into the LAN switch 11 beforehand similarly. (c) If a LAN switch creates the authentication table 16 which registers the information of the manager of said PCs 31-34 and said LAN switch 11 and the LAN switch 11 receives the packet from PC31 to PC33 to the (d) pan Learn the starting point MAC Address of a packet, a terminal point MAC Address, and a starting point IP address, and a host table 14 (drawing 2) is created. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in said host table 14 at this time, and it creates newly, or an applicable entry While being the receive port of this packet and requiring a user name and a password of PC of the starting point IP address of this packet It waits to return a user name and a password. The message which tells the purport which the rewriting

demand of a host table 14 generated to the contact mail address applicable to said starting point IP address in said authentication table 16 (the user name returned from PC into this message is put in as information.) When delivery, and the user name and password which are registered into the authentication table 16 further beforehand are not obtained (it contains also when a response is not returned in fixed time amount) While stopping entry rewriting of a host table 14, when the user name and password which discard this packet and are beforehand registered into the authentication table 16 are obtained When an applicable entry is in a key with reference to a host table 14, a terminal point IP address When a packet is outputted to an applicable port and there is no applicable entry Opt for the NeXT hop with reference to routing table (with no illustration), and an ARP table (with no illustration), and the entry of the corresponding host table 14 is created newly. The management method of the LAN switch network system characterized by outputting a packet to an applicable port is offered.

[0014] Since it can ask for the input of the user name and the password which were beforehand registered from the LAN switch 11 in that case, it becomes impossible to intercept it except PC31 which know the password [PC31], or to become and clear up it in the management method of the LAN switch network system by the 1st viewpoint of the above, although PC31 can resume automatically the same communication link as migration before even when it moves to other ports from a port 21. Moreover, since the message (put into the user name of PC32 in this message) which tells the manager of PC31 and the LAN switch 11 that is sent even when PC32 has connected the IP address of PC31 to a setup and a port 22 accidentally, the user of PC31 and the manager of the LAN switch 11 can carve the cause of a failure easily (analysis), and quick recovery becomes possible.

[0015] A communications processing means 12 by which this invention transmits and receives a packet among (a) each ports 21-25 in the 2nd viewpoint, (b) The starting point MAC Address of the packet passed from said communications processing means 12, Learn a terminal point MAC Address and a starting point IP address, and a host table 14 (drawing 2) is created. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in said host table 14 at this time, and it creates newly, or an applicable entry When it rewrites, and it asks the authentication processing means 15 whether it is good (new creation is also included), consequently the notice of the ban on rewriting is received While stopping entry rewriting of said host table 14, when this packet is discarded and the notice of rewriting authorization is received When an applicable entry is in a key with reference to said host table 14, a terminal point IP address When the packet

output to an applicable port is directed for said communications processing means 12 and there is no applicable entry Opt for the NeXT hop with reference to routing table (with no illustration), and an ARP table (with no illustration), and the entry applicable to said host table 14 is created newly. A junction processing means 13 to direct the packet output to an applicable port for said communications processing means 12, (c) If the IP address of each PCs 31-34 beforehand inputted through the administration terminal (with no illustration) etc., a user name, a password, a contact mail address, etc. are registered, the authentication table 16 is created and it is directed from said junction processing means 13 While creating the message which requires the input of a user name and a password of PC of the directed IP address and directing sending out in the receive port of this packet for said communications processing means 12 It waits to return a user name and a password. The message which tells the purport which the entry rewriting demand of a host table 14 generated to the contact mail address applicable to said IP address in said authentication table 16 (the user name returned from PC into this message is made into information) putting in -- it creating and sending out being directed for said communications processing means 12, and, when the user name and password which are registered into the authentication table 16 further beforehand are not obtained (it contains also when a response is not returned in fixed time amount) When the user name and password which notify the ban on rewriting of the entry of said host table 14 to said junction processing means 13, and are beforehand registered into the authentication table 16 are obtained The LAN switch 11 characterized by providing an authentication processing means 15 to notify rewriting authorization of the entry of said host table 14 to said junction processing means 13 is offered.

[0016] According to the LAN switch 11 by the 2nd viewpoint of the above, the management method of the LAN switch network system of the 1st viewpoint of the above can be suitably enforced now.

[0017] In the 3rd viewpoint, this invention is set on the LAN switch 11 of the above-mentioned configuration. Said authentication processing means 15 The message which requires the input of a user name and a password of PC of the IP address of the entry of the host table 14 directed from said junction processing means 13 is created. Sending out in the receive port of this packet is directed for said communications processing means 12. When the user name and password which are beforehand registered into the authentication table 16 are not obtained (it contains also when a response is not returned in fixed time amount) It not only notifies the ban on rewriting of the entry of said host table 14 to said junction processing means 13,

but The LAN switch 11 characterized by directing abandonment of all the packets that receive from the separation of a port which received this packet, or this port for said junction processing means 13 is offered.

[0018] According to the LAN switch 11 by the 3rd viewpoint of the above, the user of the setting mistake of an IP address etc. or malice can reduce the traffic load of the repeat of the input request of the user name by tapping or the thing which it is going to become and is going to communicate by clearing up, and a password using the address of other PCs.

[0019] In the 4th viewpoint, this invention is set on the LAN switch 11 of the above-mentioned configuration. Said authentication processing means 15 The message which requires the input of a user name and a password of PC of the IP address of the entry of the host table 14 directed from said junction processing means 13 is created. Sending out in the receive port of this packet is directed for said communications processing means 12. When the user name and password which are beforehand registered into the authentication table 16 are not obtained (it contains also when a response is not returned in fixed time amount) It not only notifies the ban on rewriting of the entry of said host table 14 to said junction processing means 13, but To the user of all PCs belonging to the same VLAN as the starting point IP address of this packet The message which warns of the user of the setting mistake of an IP address etc. or malice performing tapping and the communication link of spoofing using the address of other PCs is created, and the LAN switch 11 characterized by making it direct and send out to said communications processing means 12 is offered.

[0020] As another side face of the 4th viewpoint, moreover, this invention In the LAN switch 11 of the above-mentioned configuration said authentication processing means 15 The message which requires the input of a user name and a password of PC of the IP address of the entry of the host table 14 directed from said junction processing means 13 is created. The output to the receive port of this packet is directed for said communications processing means 12. Only when the user name and password which are beforehand registered into the authentication table 16 are not obtained (it contains also when a response is not returned in fixed time amount) The message which tells the purport which rewriting failure of a host table 14 generated to the contact mail address applicable to said starting point IP address in said authentication table 16 is created, and the LAN switch 11 characterized by making it direct and send out to said communications processing means 12 is offered.

[0021] According to the LAN switch 11 of the former by the 4th viewpoint of the

above, warning can be emitted in advance also to the user to whom not only a person concerned but the thing same after that may happen that the user of the setting mistake of an IP address etc. or malice is going to perform tapping and the communication link of spoofing using the address of other PCs.

[0022] Moreover, while according to the LAN switch 11 of the latter by the 4th viewpoint of the above losing the mail sent to a Shinsei (when the Shinsei user is communicating in the normal use range) user at the time of a rewriting success and reducing traffic volume, only when rewriting goes wrong, carving (analysis) and recovery of the quicker cause of a failure become possible by telling that.

[0023] In the 5th viewpoint, this invention offers the LAN switch 11 characterized by said authentication processing means 15 performing an inquiry of a user name and a password periodically not about the new creation time of the entry of a host table 14, or the time of rewriting but about each entry in the LAN switch 11 of the above-mentioned configuration.

[0024] According to the LAN switch 11 by the 5th viewpoint of the above, it can be confirmed whether have made the setting mistake of an IP address etc., or the malicious user omits tapping and the communication link of spoofing also with PC which does not send itself only by receiving a packet using the address of other PCs.

[0025] Moreover, according to the LAN switch by the 5th viewpoint of the above, it can be confirmed whether the port connection mistake the IP address setting mistake, etc. and the malicious user omit tapping and the communication link of spoofing by setting the Shinsei user's IP address as the port which PC of a user [Shinsei till then] had connected, and connecting PC.

[0026] In the 6th viewpoint, this invention is set on the LAN switch 11 of the above-mentioned configuration. Said junction processing means 13 When the new creation time of the entry of a host table 14 and rewriting applicable to the starting point IP address of a receive packet occur It not only asks said authentication processing means 15 whether I may rewrite it, but When the new creation time of the entry of a host table 14 and rewriting which correspond similarly occur also about the terminal point IP address of a receive packet, the LAN switch 11 characterized by asking said authentication processing means 15 whether I may rewrite it is offered.

[0027] According to the LAN switch 11 by the 6th viewpoint of the above, it can be confirmed whether have made the setting mistake of an IP address etc., or the malicious user omits tapping and the communication link of spoofing also with PC which does not send itself only by receiving a packet using the address of other PCs.

[0028] Moreover, according to the LAN switch by the 6th viewpoint of the above, it

can be confirmed whether the port connection mistake the IP address setting mistake, etc. and the malicious user omit tapping and the communication link of spoofing by setting the Shinsei user's IP address as the port which PC of a user [Shinsei till then] had connected, and connecting PC.

[0029]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail, referring to a drawing. In addition, thereby, this invention is not limited.

[0030] Drawing 1 is the conceptual diagram showing the configuration of the LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention, and an example of IP subnet base VLAN where the LAN switch concerned is applied. Moreover, the conceptual diagram showing an example of the various control information for which drawing 2 and drawing 3 are used with the LAN switch of the gestalt of this operation, drawing 4 , drawing 5 , and drawing 6 are flow charts which show the management method of the communication network system of the gestalt of this operation, and an example of an operation of a LAN switch.

[0031] By relaying the packet between each port 21-25 from the packet (communication link information) which received based on a host table 14 like drawing 2 learned and created, the LAN switch 11 of the gestalt of this operation realizes the communication link between PCs 31-34, and consists of a communications processing means 12, a junction processing means 13, and an authentication processing means 15.

[0032] Said communications processing means 12 is a means which transmits and receives a packet among each ports 21-25, for example, consists of electron devices, such as CPU, ASIC, RAM, and ROM.

[0033] Said junction processing means 13 is a means to relay the packet between each port 21-25 based on a host table 14, for example, consists of electron devices, such as CPU, ASIC, RAM, and ROM.

[0034] Information which shows networks, such as VLAN to which starting point IP address14a, starting point MAC Address14b, terminal point MAC Address14c, 14d of port numbers, and the port concerned belong, such as imputed network 14e, is matched, and the host table 14 is stored so that it may be illustrated by drawing 2 .

[0035] Said authentication processing means 15 is a means to perform the improper judgment which can rewrite a host table 14, for example, consists of electron devices, such as CPU, ASIC, RAM, and ROM. The information used as the radical of a

rewritable improper judgment is beforehand registered and held on the authentication table 16 (after-mentioned).

[0036] Drawing 3 is the block diagram of the authentication table 16 used with the LAN switch 11 of the gestalt of this operation. IP address 16a of PCs 31-34, user name 16b which is using the PC, password 16c, and contact mail address 16d are beforehand registered into the authentication table 16 through the console terminal (with no illustration) etc.

[0037] First, the actuation in the case of communicating from PC31 to PC33 is explained.

[0038] Drawing 4 is a flow chart which shows an example of actuation of the LAN switch 11 of the gestalt of this operation in the case of communicating from PC31 to PC33, and the management method of a communication network system.

[0039] In addition, each PCs 31-34 shall register an IP address, and the user name, a password and a contact mail address into the LAN switch 11 beforehand, the manager of the LAN switch 11 shall register a contact mail address into the LAN switch 11 beforehand similarly, and the LAN switch 11 shall have created the authentication table 16 which registers the information of the manager of said PCs 31-34 and said LAN switch 11.

[0040] PC31 creates the packet addressed to PC33, and sends it out to a port 21 (step 101).

[0041] The communications processing means 12 of the LAN switch 11 carries out reception of said packet from a port 21, and passes it to the junction processing means 13 (step 102).

[0042] The junction processing means 13 learns the starting point MAC Address of a receive packet, a terminal point MAC Address, and a starting point IP address, and creates a host table 14. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in a host table 14 at this time, and it creates newly, or an applicable entry, this entry is rewritten and it is asked to the authentication processing means 15 whether it is good (new creation is also included) (step 103). When there is no need (new creation is also included) of rewriting, it progresses to step 110. This case is a case of 1 packet eye of communication link initiation, and in order to newly create, it shall progress to degree step. It progresses to step 110 in the case after 2 packet eye.

[0043] After creating the prompt (it is called Message A.) of a user name and a password and directing sending out for the communications processing means 12, it waits for the authentication processing means 15 fixed time (step 104).

[0044] The communications processing means 12 sends out Message A to this addressing to an IP address of the receive port (port 21 in this case) of this packet (step 105).

[0045] If the communications processing means 12 receives the response message of Message A, i.e., the incoming message of a user name and a password, (it is called Message B.) from PC31, reception of it will be carried out and it will be passed to the authentication processing means 15 (step 106).

[0046] The authentication processing means 15 is a message (it is called Message C.) which tells the purport which the rewriting demand of a host table 14 generated in contact mail address 16d registered into the applicable entry of the authentication table 16 after checking that compare IP address16a currently written to be the IP address stored in Message B, a user name, and a password to the authentication table 16, user name 16b, and password 16c, and it is in agreement. into Message C, the user name stored in Message B is put in as information. creating -- the communications processing means 12 -- sending out -- directing (step 107) -- the purport of rewriting authorization is notified to the junction processing means 13 (step 109).

[0047] The communications processing means 12 sends out Message C to this addressing to a mail address (step 108).

[0048] On the other hand, if the notice of the purport of rewriting authorization is received from the authentication processing means 15, the junction processing means 13 When the applicable entry of a host table 14 is rewritten, a terminal point IP address is referred to next, a host table 14 is referred to to a key and there is an applicable entry When the packet output to an applicable port is directed for the communications processing means 12 and there is no applicable entry It opts for the NeXT hop with reference to routing table (with no illustration), and an ARP table (with no illustration), and the entry of the corresponding host table 14 is created newly, and the packet output to an applicable port is directed for the communications processing means 12 (step 110).

[0049] The communications processing means 12 sends out this packet to an applicable port (step 111).

[0050] By the above, the communication link to PC33 from PC31 can be started.

[0051] Next, after PC31 moves to a port 25 from a port 21, the actuation in the case of communicating to PC33 is explained.

[0052] Although the point as for which the entry applicable to the IP address of PC31 is already made to the host table 14 differs from the above-mentioned case, actuation carries out the same motion as the flow chart shown in drawing 4 .

[0053] PC31 creates the packet addressed to PC33, and sends it out to a port 21 (step 101).

[0054] The communications processing means 12 of the LAN switch 11 carries out reception of said packet, and passes it to the junction processing means 13 (step 102).

[0055] The junction processing means 13 learns the starting point MAC Address of a receive packet, a terminal point MAC Address, and a starting point IP address, and creates a host table 14. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in a host table 14 at this time, and it creates newly, or an applicable entry, this entry is rewritten and it is asked to the authentication processing means 15 whether it is good (new creation is also included) (step 103). When there is no need (new creation is also included) of rewriting, it progresses to step 110. This case is a case of 1 packet eye of resumption of a communication link after migration, and it shall progress to degree step in order to rewrite the information on an entry. It progresses to step 110 in the case after 2 packet eye.

[0056] After creating the prompt (it is called Message A.) of a user name and a password and directing sending out for the communications processing means 12, it waits for the authentication processing means 15 fixed time (step 104).

[0057] The communications processing means 12 sends out Message A to this addressing to an IP address of the receive port of this packet (step 105).

[0058] If the communications processing means 12 receives the response message of Message A, i.e., the incoming message of a user name and a password, (it is called Message B.), reception of it will be carried out and it will be passed to the authentication processing means 15 (step 106).

[0059] The authentication processing means 15 is a message (it is called Message C.) which tells the purport which the rewriting demand of a host table 14 generated in contact mail address 16d registered into the applicable entry of the authentication table 16 after checking that compare IP address16a currently written to be the IP address stored in Message B, a user name, and a password to the authentication table 16, user name 16b, and password 16c, and it is in agreement. into Message C, the user name stored in Message B is put in as information. creating -- the communications processing means 12 -- sending out -- directing (step 107) -- the purport of rewriting authorization is notified to the junction processing means 13 (step 109).

[0060] The communications processing means 12 sends out Message C to this addressing to a mail address (step 108).

[0061] On the other hand, if the notice of the purport of rewriting authorization is

received from the authentication processing means 15, the junction processing means 13 When the applicable entry of a host table 14 is rewritten, a terminal point IP address is referred to next, a host table 14 is referred to to a key and there is an applicable entry When the packet output to an applicable port is directed for the communications processing means 12 and there is no applicable entry It opts for the NeXT hop with reference to routing table (with no illustration), and an ARP table (with no illustration), and the entry of the corresponding host table 14 is created newly, and the packet output to an applicable port is directed for the communications processing means 12 (step 110).

[0062] The communications processing means 12 sends out this packet to an applicable port (port 25 in this case) (step 111).

[0063] By the above, PC31 can resume the communication link with PC33 also even for after migration from a port 21 automatically to a port 25.

[0064] Next, PC32 connects the IP address of PC31 to a setup and a port 22 accidentally, and the actuation at the time of starting the communication link with PC33 is explained.

[0065] Drawing 5 is a flow chart which shows an example of actuation of the LAN switch 11 of the gestalt of this operation at the time of PC32 connecting the IP address of PC31 to a setup and a port 22 accidentally, and starting the communication link with PC33, and the management method of a communication network system.

[0066] PC32 creates the packet addressed to PC33, and sends it out to a port 21 (step 121).

[0067] The communications processing means 12 of the LAN switch 11 carries out reception of said packet, and passes it to the junction processing means 13 (step 102).

[0068] The junction processing means 13 learns the starting point MAC Address of a receive packet, a terminal point MAC Address, and a starting point IP address, and creates a host table 14. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in a host table 14 at this time, and it creates newly, or an applicable entry, this entry is rewritten and it is asked to the authentication processing means 15 whether it is good (new creation is also included) (step 103). When there is no need (new creation is also included) of rewriting, it progresses to step 110. This case is a case of 1 packet eye which PC32 connected the IP address of PC31 to the setup and the port 22 accidentally, and started the communication link with PC33, and it shall progress to degree step in order to rewrite the information on an entry. In addition, in this case, since rewriting of

the information on an entry goes wrong as a result, the case after 2 packet eye will also progress to degree step.

[0069] After creating the prompt (it is called Message A.) of a user name and a password and directing sending out for the communications processing means 12, it waits for the authentication processing means 15 fixed time (step 104).

[0070] The communications processing means 12 sends out Message A to this addressing to an IP address of the receive port (port 22 in this case) of this packet (step 105).

[0071] If the communications processing means 12 receives the response message of Message A, i.e., the incoming message of a user name and a password, (it is called Message B.), reception of it will be carried out and it will be passed to the authentication processing means 15 (step 106).

[0072] The authentication processing means 15 is a message (it is called Message C.) which tells the purport which the rewriting demand of a host table 14 generated in contact mail address 16d registered into the applicable entry of the authentication table 16 after checking that compare IP address16a currently written to be the IP address stored in Message B, a user name, and a password to the authentication table 16, user name 16b, and password 16c, and it is not in agreement. into Message C, the user name stored in Message B is put in as information. creating -- the communications processing means 12 -- sending out -- directing (step 108) -- the purport of the ban on rewriting is notified to the junction processing means 13 (step 122).

[0073] The communications processing means 12 sends out Message C to this addressing to a mail address (step 108 (Message C is sent to PC31 which is the owner of Shinsei of the IP address which apologized for Message C in PC32, and was set up in this case.)).

[0074] On the other hand, if the junction processing means 13 is rewritten from the authentication processing means 15 and the notice of the purport of prohibition is received, it will stop rewriting of the applicable entry of a host table 14, and will discard this packet (step 123).

[0075] Since the message (put into the user name of PC32 which performed incorrect setting actuation into this message) which tells PC31 of Shinsei and the manager of the LAN switch 11 that is sent even when PC32 has connected the IP address of PC31 to a setup and a port 22 accidentally by the above, the user of PC31 and the manager of the LAN switch 11 can carve the cause of a failure easily, and the quick recovery of them becomes possible.

[0076] Next, a malicious user's PC35 connects the IP address of PC31 to a setup and a port 25, and the actuation at the time of starting the communication link with PC33 is explained.

[0077] Drawing 6 is a flow chart which shows an example of actuation of the LAN switch 11 of the gestalt of this operation at the time of a malicious user's PC35 connecting the IP address of PC31 to a setup and a port 25, and starting the communication link with PC33, and the management method of a communication network system.

[0078] PC35 creates the packet addressed to PC33, and sends it out to a port 25 (step 131).

[0079] The communications processing means 12 of the LAN switch 11 carries out reception of said packet, and passes it to the junction processing means 13 (step 102).

[0080] The junction processing means 13 learns the starting point MAC Address of a receive packet, a terminal point MAC Address, and a starting point IP address, and creates a host table 14. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in a host table 14 at this time, and it creates newly, or an applicable entry, this entry is rewritten and it is asked to the authentication processing means 15 whether it is good (new creation is also included) (step 103). When there is no need (new creation is also included) of rewriting, it progresses to step 110. This case is a case of 1 packet eye which a malicious user's PC35 connected the IP address of PC31 to the setup and the port 25, and started the communication link with PC33, and it shall progress to degree step in order to rewrite the information on an entry. In addition, in this case, since rewriting of the information on an entry goes wrong as a result, the case after 2 packet eye will also progress to degree step.

[0081] After creating the prompt (it is called Message A.) of a user name and a password and directing sending out for the communications processing means 12, it waits for the authentication processing means 15 fixed time (step 104).

[0082] The communications processing means 12 sends out Message A to this addressing to an IP address of the receive port (port 25 in this case) of this packet (step 105).

[0083] If the communications processing means 12 receives the response message of Message A, i.e., the incoming message of a user name and a password, (it is called Message B.), reception of it will be carried out and it will be passed to the authentication processing means 15 (step 106).

[0084] The authentication processing means 15 is a message (it is called Message C.)

which tells the purport which the rewriting demand of a host table 14 generated in contact mail address 16d registered into the applicable entry of the authentication table 16 after checking that compare IP address16a currently written to be the IP address stored in Message B, a user name, and a password to the authentication table 16, user name 16b, and password 16c, and it is not in agreement. Into Message C, the user name stored in Message B is put in as information. when Message B is not sent in the case where it is not put into a user name by Message B, or fixed time amount, the information which tells that is put in. creating -- the communications processing means 12 -- sending out -- directing (step 122) -- the purport of the ban on rewriting is notified to the junction processing means 13 (step 109).

[0085] The communications processing means 12 sends out Message C to this addressing to a mail address (step 108 (Message C reaches PC31 which is the user of Shinsei instead of PC35 of the transmitting origin of a packet in this case)).

[0086] On the other hand, if the junction processing means 13 is rewritten from the authentication processing means 15 and the notice of the purport of prohibition is received, it will stop rewriting of the applicable entry of a host table 14, and will discard this packet (step 123).

[0087] Moreover, the manager of a system who received Message C can grasp the situation based on the information stored in Message C, and can take measures.

[0088] It can prevent not performing rewriting of a host table 14, since it can ask for the input of the user name to which PC31 registered PC35 into the LAN switch 11 beforehand even if a malicious user's PC35 set up the IP address of PC31 by the above and it connected with the port 25, and a password and cannot respond correctly to it, therefore PC's35 intercepting [PC31], or becoming, and clearing up.

[0089] Next, an example other than the 1st example is explained.

[0090] In the 1st example, it sets on the LAN switch 11. The authentication processing means 15 The message A which requires the input of a user name and a password of PC of the IP address of the entry of the host table 14 directed from the junction processing means 13 is created. When the user name and password which direct sending out in the receive port of this packet for the communications processing means 12, and are beforehand registered into the authentication table 16 are not obtained (it contains also when a response is not returned in fixed time amount) Although the ban on rewriting of the entry of said host table 14 is notified to said junction processing means 13, you may make it direct abandonment of all the packets that receive from the separation (lock out) of a port which received this packet further in addition to it, or this port for said junction processing means 13. By

the above, the user of the setting mistake of an IP address etc. or malice can reduce the traffic load of the repeat of the input request of the user name by tapping or the thing which it is going to become and is going to communicate by clearing up, and a password using the address of other PCs.

[0091] In the 1st example, it sets on the LAN switch 11. Moreover, the authentication processing means 15 The message A which requires the input of a user name and a password of PC of the IP address of the entry of the host table 14 directed from the junction processing means 13 is created. When the user name and password which direct sending out in the receive port of this packet for the communications processing means 12, and are beforehand registered into the authentication table 16 are not obtained (it contains also when a response is not returned in fixed time amount) Although the ban on rewriting of the entry of said host table 14 is notified to said junction processing means 13 To the user of all PCs that furthermore belong to the same VLAN as the starting point IP address of this packet in addition to it The user of the setting mistake of an IP address etc. or malice may create the message which warns of it performing tapping and the communication link of spoofing using the address of other PCs, and may make it direct and send out to said communications processing means 12. By the above, warning can be emitted in advance also to the user to whom not only a person concerned but the thing same after that may happen that the user of the setting mistake of an IP address etc. or malice is going to perform tapping and the communication link of spoofing using the address of other PCs.

[0092] In the 1st example, it sets on the LAN switch 11. Moreover, the authentication processing means 15 Although new creation and rewriting of the entry of a host table 14 occur, it rewrites from the junction processing means 13 (new creation is included), and ** is good, or the input of a user name and a password is demanded of PC of the IP address of this entry when an inquiry is received User authentication which requires the input of a user name and a password of PC of the IP address of each entry periodically, and checks whether you are the user of Shinsei may be performed. It can be confirmed whether have made the setting mistake of an IP address etc., or, by the above, the malicious user omits tapping and the communication link of spoofing also with PC which does not send itself only by receiving a packet using the address of other PCs.

[0093] In the 1st example, it sets on the LAN switch 11. Moreover, the junction processing means 13 When the new creation time of the entry of a host table 14 and rewriting applicable to the starting point IP address of a receive packet occur It not only asks the authentication processing means 15 whether I may rewrite it, but When

the new creation time of the entry of a host table 14 and rewriting which correspond similarly occur also about the terminal point IP address of a receive packet It asks said authentication processing means 15 whether I may rewrite it, and only when rewriting authorization gets down, it may be made to rewrite this entry. It can be confirmed whether have made the setting mistake of an IP address etc., or, by the above, the malicious user omits tapping and the communication link of spoofing also with PC which does not send itself only by receiving a packet using the address of other PCs.

[0094] Moreover, although the 1st example explains using the example of IP subnet base VLAN, it is the same also at VLAN of other formats, such as the port base VLAN, the MAC Address base VLAN, and the Layer3 protocol base VLAN.

[0095] As mentioned above, according to the management method and LAN switch of each operation of a communication network, tapping and spoofing by the malicious user can be prevented and the security of a communication network system improves.

[of this invention] [of a gestalt]

[0096] Moreover, by notifying the user of Shinsei, and the manager of a system of information, such as a user name obtained in user authentication, by e-mail, the cause of a failure by the setting mistake of an IP address etc. can be easily carved now, and quick recovery becomes possible.

[0097] It will be as follows if the descriptions of this invention except having been indicated by the above-mentioned claim are enumerated.

[0098] Namely, <1> It is the management method of the communication network system constituted from a LAN switch. (a) Beforehand each PC on a LAN switch An IP address and its user name, Register a password and a contact mail address and the manager of (b) LAN switch registers a contact mail address into a LAN switch beforehand similarly. (c) If a LAN switch creates the authentication table which registers the information of the manager of said PC and said LAN switch and a LAN switch receives the packet of the communication link between each PC to the (d) pan Learn the starting point MAC Address of this packet, a terminal point MAC Address, and a starting point IP address, and a host table is created. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in said host table at this time, and it creates newly, or an applicable entry While being the receive port of this packet and requiring a user name and a password of PC of the starting point IP address of this packet Wait to return a user name and a password and the message which tells the purport which the rewriting demand of said host table generated is created. To the contact mail address which

puts in as information the user name returned from PC into this message, and corresponds to said starting point IP address in said authentication table, delivery, When a response is not returned in the case where the user name and password which are registered into said authentication table further beforehand are not obtained, or fixed time amount While stopping entry rewriting of said host table, when the user name and password which discard this packet and are beforehand registered into said authentication table are obtained When an applicable entry is in a key with reference to said host table, a terminal point IP address It is the management method of the communication network system characterized by creating the entry of the corresponding host table newly and outputting a packet to an applicable port when a packet is outputted to an applicable port and there is no applicable entry.

[0099] <2> In the management method of the communication network system of the aforementioned <1> publication a LAN switch When a response is not returned in the case where the user name and password which are beforehand registered into said authentication table are not obtained, or fixed time amount stopping entry rewriting of said host table and discarding this packet -- in addition, the management method of the communication network system characterized by performing all packet abandonment that receives from the separation of a port which received this packet further, or this port.

[0100] <3> In the management method of the communication network system of the aforementioned <1> publication a LAN switch When a response is not returned in the case where the user name and password which are beforehand registered into said authentication table are not obtained, or fixed time amount Stop entry rewriting of said host table and it adds to discarding this packet. To the user of all PCs that furthermore belong to the same VLAN as the starting point IP address of this packet The management method of the communication network system characterized by creating and sending the message which warns of the user of the setting mistake of an IP address etc. or malice performing tapping and the communication link of spoofing using the address of other PCs.

[0101] <4> in the management method of the communication network system of the aforementioned <1> publication, a LAN switch requires the input of a user name and a password of PC of the IP address of this entry, when the entry new creation time of a host table and rewriting occur -- in addition, management method of the communication network system characterized by requiring the input of a user name and a password of PC of the IP address of each entry still more nearly periodically.

[0102] <5> In the management method of the communication network system of the

aforementioned <1> publication a LAN switch It adds to requiring the input of a user name and a password of PC of the IP address of this entry, when the new creation time of the entry of a host table and rewriting applicable to the starting point IP address of a receive packet occur. When the new creation time of the entry of a host table and rewriting which furthermore correspond to the terminal point IP address of this packet occur, the input of a user name and a password is required of PC of the IP address of this entry. The management method of the communication network system characterized by rewriting this entry only when the user name and password which are beforehand registered into the authentication table are obtained about a terminal point IP address as well as a starting point IP address.

[0103] <6> The communications processing means which transmits and receives a packet between (a) each port, (b) The starting point MAC Address of the packet passed from said communications processing means, Learn a terminal point MAC Address and a starting point IP address, and a host table is created. When rewriting to different information from the case where there is no entry which corresponds to said starting point IP address in said host table at this time, and it creates newly, or an applicable entry When it asks an authentication processing means whether I may new-create or may rewrite, consequently the notice of the ban on rewriting is received While stopping entry rewriting of said host table, when this packet is discarded and the notice of rewriting authorization is received When an applicable entry is in a key with reference to said host table, a terminal point IP address When the packet output to an applicable port is directed for said communications processing means and there is no applicable entry A junction processing means to create the entry applicable to said host table newly, and to direct the packet output to an applicable port for said communications processing means, (c) If the IP address of each PC beforehand inputted through the administration terminal etc., a user name, a password, a contact mail address, etc. are registered, an authentication table is created and it is directed from said junction processing means While creating the message which requires the input of a user name and a password of PC of the directed IP address and directing sending out in the receive port of said packet for said communications processing means Wait to return a user name and a password and the message which tells the purport which the entry rewriting demand of said host table generated to the contact mail address applicable to said IP address in said authentication table is created. Put in as information the user name returned from PC into this message, and sending out is directed for said communications processing means. When a response is not returned in the case where the user name and

password which are registered into said authentication table further beforehand are not obtained, or fixed time amount When the user name and password which notify the ban on rewriting of the entry of said host table to said junction processing means, and are beforehand registered into the authentication table are obtained The LAN switch characterized by providing an authentication processing means to notify rewriting authorization of the entry of said host table to said junction processing means.

[0104] <7> It is the management method of the communication network system constituted from a LAN switch. (a) Beforehand each PC on a LAN switch A MAC Address and its user name, Register a password and a contact mail address and the manager of (b) LAN switch registers a contact mail address into a LAN switch beforehand similarly. (c) If a LAN switch creates the authentication table which registers the information of the manager of said PC and said LAN switch and a LAN switch receives the packet of the communication link between each PC to the (d) pan Learn the starting point MAC Address of this packet, and a host table is created. When rewriting to different information from the case where there is no entry which corresponds in said host table at said starting point MAC Address at this time, and it creates newly, or an applicable entry While being the receive port of this packet and requiring a user name and a password of PC of the starting point MAC Address of this packet Wait to return a user name and a password and the message which tells the purport which the rewriting demand of said host table generated is created. To the contact mail address which puts in as information the user name returned from PC into this message, and corresponds to said starting point MAC Address in said authentication table, delivery, When a response is not returned in the case where the user name and password which are registered into said authentication table further beforehand are not obtained, or fixed time amount While stopping entry rewriting of said host table, when the user name and password which discard this packet and are beforehand registered into said authentication table are obtained When an applicable entry is in a key with reference to said host table, a terminal point MAC Address It is the management method of the communication network system characterized by creating the entry of the corresponding host table newly and outputting a packet to an applicable port when a packet is outputted to an applicable port and there is no applicable entry.

[0105] Although invention made by this invention person above was concretely explained based on the gestalt of operation, it cannot be overemphasized that it can change variously in the range which this invention is not limited to the gestalt of said operation, and does not deviate from the summary.

[0106]

[Effect of the Invention] According to the management method of the communication network system of this invention, the effectiveness that prevention of the poor communication link by the setting mistake of a logical or physical network address etc., and the cause analysis of a poor communication link and speeding up of recovery operation are attained is acquired.

[0107] Moreover, according to the management method of the communication network system of this invention, the effectiveness that the security of a communication network can be raised by preventing tapping and spoofing by the malicious user is acquired.

[0108] According to the information repeating installation of this invention, the effectiveness that prevention of the poor communication link by the setting mistake of a logical or physical network address etc., the analysis of a poor communication link, and speeding up of recovery operation are attained is acquired.

[0109] Moreover, according to the information repeating installation of this invention, the effectiveness that the security of a communication network system can be raised by preventing tapping and spoofing by the malicious user is acquired.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the conceptual diagram showing an example of the configuration of a LAN switch which enforces the management method of the communication network

system which is the 1st operation gestalt of this invention.

[Drawing 2] It is the conceptual diagram showing an example of the host table used with the LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention.

[Drawing 3] It is the conceptual diagram showing an example of the authentication table used with the LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention.

[Drawing 4] It is the flow chart which shows an example of an operation of a LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention.

[Drawing 5] It is the flow chart which shows an example of an operation of a LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention.

[Drawing 6] It is the flow chart which shows an example of an operation of a LAN switch which enforces the management method of the communication network system which is the 1st operation gestalt of this invention.

[Drawing 7] It is the conceptual diagram showing an example of IP subnet base VLAN which is the reference technique of this invention.

[Description of Notations]

11 -- A LAN switch (information repeating installation), 12 -- Communications processing means (control logic), 13 -- A junction processing means (control logic), 14 -- Host table (control table), 14a -- A starting point IP address, 14b -- A starting point MAC Address, 14c -- Terminal point MAC Address, 14d -- A port number, 14e -- An imputed network, 15 -- Authentication processing means (control logic), 16 [-- A password, 16d / -- A contact mail address, 21-25 / -- A port (input/output port) 31-34, 35 --PC, A B, C / -- Message.] -- An authentication table, 16a -- An IP address, 16b -- A user name, 16c

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－174796
（P2000－174796A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ 12/46		Ｈ０４Ｌ 11/00	３１０Ｃ	５Ｊ１０４
12/28		9/00	６７５Ａ	５Ｋ０３０
9/32		11/20	Ｂ	５Ｋ０３３
12/66			１０２Ｄ	５Ｋ０３５
12/56		13/00	３１１	９Ａ００１

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平10－347235
(22)出願日　平成10年12月７日(1998.12.7)

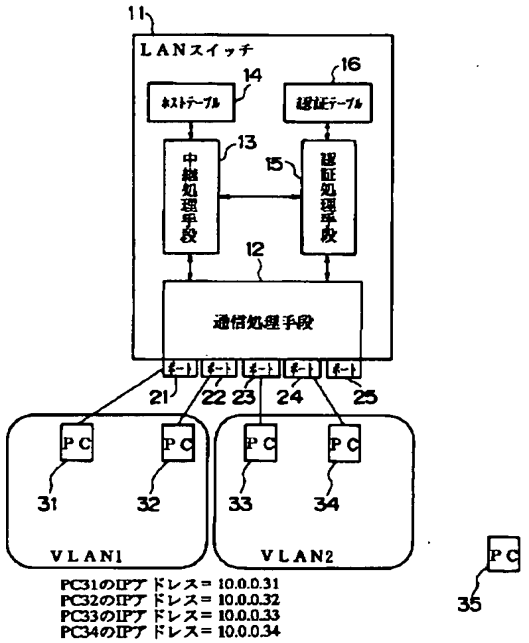
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　土屋　一暁
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(72)発明者　野崎　信司
神奈川県海老名市下今泉810番地　株式会社日立製作所サーバ開発本部内
(74)代理人　100080001
弁理士　筒井　大和

最終頁に続く

(54)【発明の名称】　通信ネットワークシステムの管理方法および情報中継装置

(57)【要約】
【課題】　悪意のユーザによる盗聴やなりすましの防止、アドレス設定ミスの解析や回復を容易にする。
【解決手段】　複数のポート２１～２５の各々に任意にネットワーク端末としての複数のＰＣ３１～３４を接続することでＶＬＡＮ１およびＶＬＡＮ２等の通信ネットワークを構成するＬＡＮスイッチ１１において、各ポート２１～２５との間でパケットの送受信を行う通信処理手段１２と、各ポートと、接続されたＰＣのアドレス情報との対応関係の変化を学習して更新されるホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行う中継処理手段１３と、パケット中継契機のホストテーブル１４の更新時に、認証テーブル１６を参照して送信元のＰＣに対してユーザ認証を行い、真正のユーザの場合にのみホストテーブル１４の書き換えおよびパケットの中継を許可する認証処理手段１５とを備えた。

図　1



1

【特許請求の範囲】

【請求項１】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置を用いた通信ネットワークシステムの管理方法であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードとが対応付けて格納された認証テーブルを設定する第１のステップと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方のユーザに対して、前記ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードと照合するユーザ認証を実行し、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する第２のステップと、

を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項２】　請求項１記載の通信ネットワークシステムの管理方法において、

前記第１のステップでは、前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方に対して、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスも対応付けて設定し、前記第２のステップでは、前記ユーザ認証にて前記通信情報の送信元または送信先の前記ユーザから入力された前記ユーザ名を含むとともに前記制御テーブルの更新要求が発生したことを通知するメッセージを作成して該当する前記ネットワーク論理アドレスまたはネットワーク物理アドレスの前記ユーザおよび管理者の少なくとも一方の連絡先メールアドレスに対して送出する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに当該通信情報を受信した前記入出力ポートの切り離し、および当該入出力ポートから受信した全ての通信情報を廃棄する処理、

前記第２のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに該通信情報の送信元の前記ネットワーク論理アドレスまたはネットワーク物理アドレスと同一の仮想ＬＡＮ（ローカル・エリア・ネットワーク）に属す全ての前記ネットワーク端末のユーザに、前記ネットワーク論理アドレスまたはネットワーク物理アドレス等の設定ミスや、悪意のユーザが他のネットワーク端末のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送る処理、

前記制御テーブルの更新要求発生の有無に関係なく、定期的または不定期に前記制御テーブル内に登録された前記ネットワーク論理アドレスまたはネットワーク物理アドレスのユーザに対して前記ユーザ認証を実行する処理、

の少なくとも一つの処理を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項３】　ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードと、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスが対応付けて格納された認証テーブルと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方の前記ユーザに対して、ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およ

びパスワードと照合するユーザ認証を実行するとともに、前記通信情報の送信元および前記管理者の少なくとも一方の前記連絡先メールアドレスに対して前記ユーザ認証で得られた前記ユーザ名と前記制御テーブルの更新要求が発生したことを通知するメッセージを送信するとともに、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する動作を行う制御論理と、

を備えたことを特徴とする情報中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信ネットワークシステムの管理技術および情報中継技術に関し、特に、ＬＡＮ(LAN: Local Area Network) スイッチ(Layer2 スイッチ、Layer3スイッチ等) と呼ばれるインタネットワーク装置、およびＬＡＮスイッチで構成する通信ネットワークシステム（ＬＡＮスイッチネットワークシステム）の管理方法等に適用して有効な技術に関する。

【０００２】

【従来の技術】ＬＡＮスイッチが有する特徴技術にＶＬＡＮ(VLAN: Virtual LAN) がある。ＶＬＡＮはインタネットワーク装置の物理的なポートに依存せずにＬＡＮの構築を可能にする技術であり、その形式の違いによってポートベースＶＬＡＮ、ＭＡＣ(MAC: Media Access Control) アドレスベースＶＬＡＮ、Layer3プロトコルベースＶＬＡＮ、ＩＰ(IP: Internet Protocol) サブネットベースＶＬＡＮ等の名称で知られている。

【０００３】本発明の参考技術では、例えば図７に示すＩＰサブネットベースＶＬＡＮの通信ネットワークシステムにおいて複数のポート２２１～２２５を備えたＬＡＮスイッチ２１０はＰＣ(PC: Personal Computer) ２３１からＰＣ２３３へのパケットを受信すると、パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル２２０を作成する。次に終点ＩＰアドレスをキーにホストテーブル２２０を参照し、該当エントリが有る場合は、該当ポートにパケットを出力する。該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰ(ARP: Address Resolution Protocol)テーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル２２０のエントリを新規に作成して、該当ポートにパケットを出力する。ＬＡＮスイッチ２１０はこのようにしてＰＣ２３１からＰＣ２３３へのパケットを中継する。

【０００４】さらにＬＡＮスイッチ２１０では、定期的にホストテーブル２２０のエントリを廃棄し、新たにパケットから学習することによって常にホストテーブル２２０のエントリを更新しているため、ＰＣが移動した場合でも移動先のポートにパケットを正しく中継すること

ができる。すなわちＰＣは移動した場合でも移動前と同様の通信を自動的に再開することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、上記参考技術には、次の技術的課題がある。

【０００６】第１の技術的課題は、ＩＰアドレス等の設定ミスに対して無防備なことである。例えばＰＣ２３２がＰＣ２３１のＩＰアドレスを誤って設定、ポート２２２に接続してしまったとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２２に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＩＰアドレスを正しく使用しているＰＣ２３１が通信出来なくなる等の通信不良が発生する。また、ネットワークに接続されるＰＣの数が多い場合には、この通信不良の解析や回復には、多大の労力を要する。

【０００７】第２の技術的課題は、悪意のユーザによる盗聴やなりすましを許してしまうことである。例えばＰＣ２３５がＰＣ２３１のＩＰアドレスを設定、ポート２２５に接続したとする。この場合、ＬＡＮスイッチ２１０ではＰＣ２３１がポート２２１からポート２２５に移動したと判断し、そのようにホストテーブル２２０を書き換えてしまう。この結果、ＰＣ２３５がＰＣ２３１宛の通信データを受け取って盗聴したり、またＰＣ２３１になりすまして通信できてしまう。

【０００８】本発明の目的は、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【０００９】本発明の他の目的は、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることが可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【００１０】

【課題を解決するための手段】本発明は、ＬＡＮスイッチ等の情報中継装置に備えられた複数の入出力ポートにユーザ端末や他の中継装置を接続して構築され、入出力ポートに対するユーザ端末等の接続状態の変化を学習して、入出力ポートとネットワークアドレスとの対応関係を管理する制御テーブルを更新することで、個々のユーザ端末の入出力ポートに対する接続状態を動的に変更することが可能な通信ネットワークの管理方法において、各ユーザ端末間、すなわち複数の入出力ポート間で通信情報の授受を契機とする制御テーブルの更新要求が発生した時、当該通信情報の送信元のユーザ端末に対してユーザ認証を実行し、真正のユーザであることが確認された場合にのみ、制御テーブルの更新およびそれに基づく通信情報の授受を行わせるものである。

【００１１】また、各ユーザ端末およびシステム管理者の連絡先メールアドレスを、ユーザ認証に用いられるネットワークアドレスやユーザ名、パスワード等が格納された認証テーブルの一部に登録しておき、制御テーブルの更新要求の発生時に、当該更新要求が発生したことを記したメッセージを通信情報の送信元のユーザ端末やシステム管理者等にメールで送るものである。この際、ユーザ認証の成功の有無に関係なく、当該ユーザ認証にて得られたユーザ名を当該メッセージ内に格納する。

【００１２】より具体的には、本発明は、以下の特徴を有する。

【００１３】第１の観点では、本発明は、ＬＡＮスイッチで構成する通信ネットワークシステムにおいて、ＩＰアドレス等の設定ミスによる通信不良、悪意のユーザによる盗聴やなりすましを防ぐことができるＬＡＮスイッチネットワークシステムの管理方法であって、例えば図１に示すＩＰサブネットベースＶＬＡＮの通信ネットワークシステムにおいて、（ａ）ＰＣ３１～３４はＬＡＮスイッチ１１に予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチ１１の管理者も同様にＬＡＮスイッチ１１に予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣ３１～３４および前記ＬＡＮスイッチ１１の管理者の情報を登録する認証テーブル１６を作成し、（ｄ）さらにＬＡＮスイッチ１１はＰＣ３１からＰＣ３３へのパケットを受信すると、パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４（図２）を作成し、このとき前記ホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＩＰアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル１６の中の前記始点ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中にＰＣから返されたユーザ名を情報として入れる。）を送り、さらに予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、ホストテーブル１４のエントリ書き換えを中止するとともに該パケットを廃棄し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られた場合は、終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートにパケットを出力することを特徴とするＬＡＮスイッチネットワークシステムの管理方法を提供する。

【００１４】上記第１の観点によるＬＡＮスイッチネットワークシステムの管理方法では、ＰＣ３１はポート２１から他のポートに移動した場合でも移動前と同様の通信を自動的に再開することができるが、その際、ＬＡＮスイッチ１１から予め登録したユーザ名とパスワードの入力を求められるため、そのパスワードを知っているＰＣ３１以外がＰＣ３１を装って盗聴したり、なりすましたりすることが出来なくなる。またＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまった場合でも、ＰＣ３１およびＬＡＮスイッチ１１の管理者にその旨を伝えるメッセージ（本メッセージの中にＰＣ３２のユーザ名が入れられている）が送られるので、ＰＣ３１のユーザやＬＡＮスイッチ１１の管理者は容易に障害原因の切り分け（解析）を行うことができ、迅速な回復処理が可能になる。

【００１５】第２の観点では、本発明は、（ａ）各ポート２１～２５との間でパケットの送受信を行う通信処理手段１２と、（ｂ）前記通信処理手段１２から渡されたパケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４（図２）を作成し、このとき前記ホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブル１４のエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点ＩＰアドレスをキーに前記ホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、前記ホストテーブル１４に該当するエントリを新規に作成して、該当ポートへのパケット出力を前記通信処理手段１２に指示する中継処理手段１３と、（ｃ）予め管理端末（図示無し）等を介して入力された各ＰＣ３１～３４のＩＰアドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブル１６を作成し、前記中継処理手段１３から指示されると、指示されたＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブル１６の中の前記ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４のエントリ書き換え要求が発生した旨を伝えるメッセージ（本メッセージの中にＰＣから返されたユーザ名を情報として入れる）を作成して前記

通信処理手段１２に送出を指示し、さらに予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブル１４のエントリの書き換え許可を前記中継処理手段１３に通知する認証処理手段１５とを具備したことを特徴とするＬＡＮスイッチ１１を提供する。

【００１６】上記第２の観点によるＬＡＮスイッチ１１によれば、上記第１の観点のＬＡＮスイッチネットワークシステムの管理方法を好適に実施できるようになる。

【００１７】第３の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知するだけでなく、該パケットを受信したポートの切り離しや該ポートから受信する全てのパケットの廃棄を前記中継処理手段１３に指示することを特徴とするＬＡＮスイッチ１１を提供する。

【００１８】上記第３の観点によるＬＡＮスイッチ１１によれば、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

【００１９】第４の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの送出を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知するだけでなく、該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段１２に指示して送出させることを特徴とするＬＡＮスイッチ１１を提供する。

【００２０】また、第４の観点の別の側面として、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、前記中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、該パケットの受信ポートへの出力を前記通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）のみ、前記認証テーブル１６の中の前記始点ＩＰアドレスに該当する連絡先メールアドレスにホストテーブル１４の書き換え失敗が発生した旨を伝えるメッセージを作成して、前記通信処理手段１２に指示して送出させることを特徴とするＬＡＮスイッチ１１を提供する。

【００２１】上記第４の観点による前者のＬＡＮスイッチ１１によれば、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

【００２２】また上記第４の観点による後者のＬＡＮスイッチ１１によれば、書き換え成功時（真正なユーザが正常な使用範囲で通信している場合）に真正なユーザに送られてくるメールを無くしてトラヒック量を減らすとともに、書き換えに失敗する場合のみ、その旨を伝えることによって、より迅速な障害原因の切り分け（解析）および回復処理が可能となる。

【００２３】第５の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記認証処理手段１５は、ホストテーブル１４のエントリの新規作成時や書き換え時ではなく、各エントリについて定期的にユーザ名とパスワードの問い合わせを行うことを特徴とするＬＡＮスイッチ１１を提供する。

【００２４】上記第５の観点によるＬＡＮスイッチ１１によれば、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２５】また上記第５の観点によるＬＡＮスイッチによれば、ポート接続ミス・ＩＰアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのＰＣが接続していたポートに、その真正なユーザのＩＰアドレスを設定してＰＣを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２６】第６の観点では、本発明は、上記構成のＬＡＮスイッチ１１において、前記中継処理手段１３は、受信パケットの始点ＩＰアドレスに該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせるだけでなく、受信パケットの終点ＩＰア

ドレスについても同様に、該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせることを特徴とするＬＡＮスイッチ１１を提供する。

【００２７】上記第６の観点によるＬＡＮスイッチ１１によれば、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２８】また上記第６の観点によるＬＡＮスイッチによれば、ポート接続ミス・ＩＰアドレス設定ミス等や、悪意のユーザが、それまで真正なユーザのＰＣが接続していたポートに、その真正なユーザのＩＰアドレスを設定してＰＣを接続し、盗聴やなりすましの通信を行っていないかチェックすることができる。

【００２９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。なお、これにより本発明が限定されるものではない。

【００３０】図１は、本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの構成、および当該ＬＡＮスイッチが適用されるＩＰサブネットベースＶＬＡＮの一例を示す概念図である。また、図２および図３は、本実施の形態のＬＡＮスイッチにて用いられる各種制御情報の一例を示す概念図、図４、図５および図６は、本実施の形態の通信ネットワークシステムの管理方法およびＬＡＮスイッチの作用の一例を示すフローチャートである。

【００３１】本実施の形態のＬＡＮスイッチ１１は、受信したパケット（通信情報）から学習して作成した図２のようなホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行うことにより、ＰＣ３１～３４の間の通信を実現するものであり、通信処理手段１２と、中継処理手段１３と、認証処理手段１５とから構成される。

【００３２】前記通信処理手段１２は、各ポート２１～２５との間でパケットの送受信を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。

【００３３】前記中継処理手段１３は、ホストテーブル１４に基づき各ポート２１～２５間のパケットの中継を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。

【００３４】図２に例示されるように、ホストテーブル１４は、始点ＩＰアドレス１４ａ、始点ＭＡＣアドレス１４ｂ、終点ＭＡＣアドレス１４ｃ、ポート番号１４ｄ、当該ポートが帰属するＶＬＡＮ等のネットワークを示す帰属ネットワーク１４ｅ、等の情報が対応付けられて格納されている。

【００３５】前記認証処理手段１５は、ホストテーブル１４の書き換え可不可の判定を行う手段であり、例えばＣＰＵ、ＡＳＩＣ、ＲＡＭ、ＲＯＭ等の電子デバイスで構成される。書き換え可不可の判定の基となる情報は認証テーブル１６（後述）に予め登録、保持している。

【００３６】図３は、本実施の形態のＬＡＮスイッチ１１にて用いられる認証テーブル１６の構成図である。認証テーブル１６には、ＰＣ３１～３４のＩＰアドレス１６ａと、そのＰＣを使用しているユーザ名１６ｂ、パスワード１６ｃ、連絡先メールアドレス１６ｄが予めコンソール端末（図示無し）等を介して登録されている。

【００３７】先ず、ＰＣ３１からＰＣ３３に通信する場合の動作について説明する。

【００３８】図４は、ＰＣ３１からＰＣ３３に通信する場合の本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００３９】なお各ＰＣ３１～３４はＬＡＮスイッチ１１に予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、ＬＡＮスイッチ１１の管理者も同様にＬＡＮスイッチ１１に予め連絡先メールアドレスを登録し、ＬＡＮスイッチ１１は前記ＰＣ３１～３４および前記ＬＡＮスイッチ１１の管理者の情報を登録する認証テーブル１６を作成してあるものとする。

【００４０】ＰＣ３１は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１０１）。

【００４１】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットをポート２１から受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００４２】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは通信開始の１パケット目のケースであり、新規作成するため次ステップに進むものとする。２パケット目以降のケースではステップ１１０に進む。

【００４３】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００４４】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２１）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００４５】通信処理手段１２は、メッセージＡの応答

メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）をＰＣ３１から受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００４６】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致することを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０７）とともに、書き換え許可の旨を中継処理手段１３に通知する（ステップ１０９）。

【００４７】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（ステップ１０８）。

【００４８】一方、中継処理手段１３は、認証処理手段１５から書き換え許可の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを行い、次に終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段１２に指示する（ステップ１１０）。

【００４９】通信処理手段１２は、該パケットを該当ポートに送出する（ステップ１１１）。

【００５０】以上により、ＰＣ３１からＰＣ３３への通信を開始することが出来る。

【００５１】次にＰＣ３１がポート２１からポート２５に移動した後、ＰＣ３３に通信する場合の動作について説明する。

【００５２】ＰＣ３１のＩＰアドレスに該当するエントリが既にホストテーブル１４にできている点が前述のケースと異なるが、動作は図４に示すフローチャートと同じ動きをする。

【００５３】ＰＣ３１は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１０１）。

【００５４】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００５５】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは移動後の通信再開の１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。２パケット目以降のケースではステップ１１０に進む。

【００５６】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００５７】通信処理手段１２は、メッセージＡを該パケットの受信ポートの該ＩＰアドレス宛に送出する（ステップ１０５）。

【００５８】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００５９】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致することを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０７）とともに、書き換え許可の旨を中継処理手段１３に通知する（ステップ１０９）。

【００６０】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（ステップ１０８）。

【００６１】一方、中継処理手段１３は、認証処理手段１５から書き換え許可の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを行い、次に終点ＩＰアドレスをキーにホストテーブル１４を参照し、該当エントリが有る場合は、該当ポートへのパケット出力を通信処理手段１２に指示し、該当エントリが無い場合は、ルーティングテーブル（図示無し）およびＡＲＰテーブル（図示無し）を参照してネクストホップを決め、該当するホストテーブル１４のエントリを新規に作成して、該当ポートへのパケット出力を通信処理手段１２に指示する（ステップ１１０）。

【００６２】通信処理手段１２は、該パケットを該当ポート（この場合、ポート２５）に送出する（ステップ１１１）。

【００６３】以上により、ＰＣ３１はポート２１からポート２５へ移動後も、ＰＣ３３との通信を自動的に再開することが出来る。

【００６４】次にＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した場合の動作について説明する。

【００６５】図５は、ＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した場合における、本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００６６】ＰＣ３２は、ＰＣ３３宛のパケットを作成してポート２１に送出する（ステップ１２１）。

【００６７】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００６８】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースはＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまい、ＰＣ３３との通信を開始した１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、２パケット目以降のケースも次ステップに進むことになる。

【００６９】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００７０】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２２）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００７１】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００７２】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致していないことを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１０８）とともに、書き換え禁止の旨を中継処理手段１３に通知する（ステップ１２２）。

【００７３】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（この場合、メッセージＣは、ＰＣ３２において謝って設定されたＩＰアドレスの真正の所有者であるＰＣ３１宛にメッセージＣが送られる。）（ステップ１０８）。

【００７４】一方、中継処理手段１３は、認証処理手段１５から書き換え禁止の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを中止し、該パケットを廃棄する（ステップ１２３）。

【００７５】以上により、ＰＣ３２がＰＣ３１のＩＰアドレスを誤って設定、ポート２２に接続してしまった場合でも、真正のＰＣ３１およびＬＡＮスイッチ１１の管理者にその旨を伝えるメッセージ（本メッセージの中に誤設定操作を行ったＰＣ３２のユーザ名が入れられている）が送られるので、ＰＣ３１のユーザやＬＡＮスイッチ１１の管理者は容易に障害原因の切り分けを行うことができ、迅速な回復処理が可能となる。

【００７６】次に悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した場合の動作について説明する。

【００７７】図６は、悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した場合における、本実施の形態のＬＡＮスイッチ１１および通信ネットワークシステムの管理方法の動作の一例を示すフローチャートである。

【００７８】ＰＣ３５は、ＰＣ３３宛のパケットを作成してポート２５に送出する（ステップ１３１）。

【００７９】ＬＡＮスイッチ１１の通信処理手段１２は、前記パケットを受信処理して中継処理手段１３に渡す（ステップ１０２）。

【００８０】中継処理手段１３は、受信パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブル１４を作成する。このときホストテーブル１４の中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該エントリを書き換えて（新規作成も含む）良いか認証処理手段１５に問い合わせる（ステップ１０３）。書き換える必要（新規作成も含む）が無い場合はステップ１１０に進む。本ケースは悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定、ポート２５に接続し、ＰＣ３３との通信を開始した１パケット目のケースであり、エントリの情報を書き換えるため次ステップに進むものとする。なお本ケースでは結果としてエントリの情報の書き換えに失敗するため、２パケット目以降のケースも次ステップに進むことになる。

【００８１】認証処理手段１５は、ユーザ名とパスワードの入力要求メッセージ（メッセージＡと呼ぶ。）を作

成して通信処理手段１２に送出を指示した後、一定時間待つ（ステップ１０４）。

【００８２】通信処理手段１２は、メッセージＡを該パケットの受信ポート（この場合、ポート２５）の該ＩＰアドレス宛に送出する（ステップ１０５）。

【００８３】通信処理手段１２は、メッセージＡの応答メッセージ、すなわちユーザ名とパスワードの入力メッセージ（メッセージＢと呼ぶ。）を受信すると、受信処理して認証処理手段１５に渡す（ステップ１０６）。

【００８４】認証処理手段１５は、メッセージＢに格納されているＩＰアドレス、ユーザ名、パスワードと、認証テーブル１６に書かれているＩＰアドレス１６ａ、ユーザ名１６ｂ、パスワード１６ｃを比較して一致していないことを確認した後、認証テーブル１６の該当エントリに登録されている連絡先メールアドレス１６ｄにホストテーブル１４の書き換え要求が発生した旨を伝えるメッセージ（メッセージＣと呼ぶ。メッセージＣの中にはメッセージＢに格納されているユーザ名を情報として入れる。メッセージＢにユーザ名が入れられてない場合や一定時間内にメッセージＢが送られてこなかった場合はその旨を伝える情報を入れる。）を作成して通信処理手段１２に送出を指示する（ステップ１２２）とともに、書き換え禁止の旨を中継処理手段１３に通知する（ステップ１０９）。

【００８５】通信処理手段１２は、メッセージＣを該メールアドレス宛に送出する（この場合、メッセージＣは、パケットの送信元のＰＣ３５ではなく、真正のユーザであるＰＣ３１に届く）（ステップ１０８）。

【００８６】一方、中継処理手段１３は、認証処理手段１５から書き換え禁止の旨の通知を受けると、ホストテーブル１４の該当エントリの書き換えを中止し、該パケットを廃棄する（ステップ１２３）。

【００８７】また、メッセージＣを受け取ったシステムの管理者は、メッセージＣに格納されている情報に基づいて事態を把握し、対策をとることができる。

【００８８】以上により、悪意のユーザのＰＣ３５がＰＣ３１のＩＰアドレスを設定し、ポート２５に接続しても、ＰＣ３５は予めＰＣ３１がＬＡＮスイッチ１１に登録したユーザ名とパスワードの入力を求められ、それに正しく応えられないため、ホストテーブル１４の書き換えは行われず、したがってＰＣ３５がＰＣ３１を装って盗聴したり、なりすましたりすることを防ぐことができる。

【００８９】次に、第１の実施例とは別の実施例について説明する。

【００９０】第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージＡを作成して、該パケットの受信ポートへの送出を通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知しているが、さらにそれに加えて該パケットを受信したポートの切り離し（閉塞）や該ポートから受信する全てのパケットの廃棄を前記中継処理手段１３に指示するようにしても良い。以上により、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすまして通信を行おうとすることによるユーザ名とパスワードの入力要求の繰り返しのトラヒック負荷を減らすことができる。

【００９１】また、第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、中継処理手段１３から指示されたホストテーブル１４のエントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージＡを作成して、該パケットの受信ポートへの送出を通信処理手段１２に指示し、予め認証テーブル１６に登録されているユーザ名とパスワードが得られなかった場合（一定時間内に応答が返されなかった場合も含む）は、前記ホストテーブル１４のエントリの書き換え禁止を前記中継処理手段１３に通知しているが、さらにそれに加えて該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して、前記通信処理手段１２に指示して送出させても良い。以上により、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしていることを、当事者だけでなく、その後同じ事が起きる可能性があるユーザにも事前に警告を発することができる。

【００９２】また、第１の実施例ではＬＡＮスイッチ１１において、認証処理手段１５は、ホストテーブル１４のエントリの新規作成や書き換えが発生し、中継処理手段１３から書き換え（新規作成を含む）て良いか問い合わせを受けた時に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求しているが、定期的に各エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求して真正のユーザか否かを確認するユーザ認証を行っても良い。以上により、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００９３】また、第１の実施例ではＬＡＮスイッチ１１において、中継処理手段１３は、受信パケットの始点ＩＰアドレスに該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き

換えて良いか認証処理手段１５に問い合わせるだけでなく、受信パケットの終点ＩＰアドレスについても同様に、該当するホストテーブル１４のエントリの新規作成時や書き換えが発生した場合に、それを書き換えて良いか前記認証処理手段１５に問い合わせ、書き換え許可がおりた場合のみ該エントリの書き換えを行うようにしても良い。以上により、パケットを受信するのみで自ら発信を行わないＰＣについても、ＩＰアドレス等の設定ミスをしていないか、悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行っていないかチェックすることができる。

【００９４】また、第１の実施例ではＩＰサブネットベースＶＬＡＮの例を用いて説明しているが、ポートベースＶＬＡＮ、ＭＡＣアドレスベースＶＬＡＮ、Layer3プロトコルベースＶＬＡＮ等の他の形式のＶＬＡＮでも同様である。

【００９５】以上のように、本発明の各実施の形態の通信ネットワークの管理方法およびＬＡＮスイッチによれば、悪意のユーザによる盗聴やなりすましを防ぐことができ、通信ネットワークシステムのセキュリティが向上する。

【００９６】また、ユーザ認証にて得られたユーザ名等の情報を真正のユーザやシステムの管理者にメールで通知することにより、ＩＰアドレス等の設定ミスによる障害原因を容易に切り分けられるようになり、迅速な回復処理が可能になる。

【００９７】上記した特許請求の範囲に記載された以外の本発明の特徴を列挙すれば以下の通りである。

【００９８】すなわち、

＜１＞　ＬＡＮスイッチで構成する通信ネットワークシステムの管理方法であって、（ａ）各ＰＣはＬＡＮスイッチに予めＩＰアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチの管理者も同様にＬＡＮスイッチに予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣおよび前記ＬＡＮスイッチの管理者の情報を登録する認証テーブルを作成し、（ｄ）さらにＬＡＮスイッチは各ＰＣ間の通信のパケットを受信すると、該パケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＩＰアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記認証テーブルの中の前記始点ＩＰアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点ＩＰアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

【００９９】＜２＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットを受信したポートの切り離しや該ポートから受信する全てのパケット廃棄を行うことを特徴とする通信ネットワークシステムの管理方法。

【０１００】＜３＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合に、前記ホストテーブルのエントリ書き換えを中止し、該パケットを廃棄することに加えて、さらに該パケットの始点ＩＰアドレスと同一ＶＬＡＮに属す全てのＰＣのユーザに、ＩＰアドレス等の設定ミスや悪意のユーザが他のＰＣのアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送ることを特徴とする通信ネットワークシステムの管理方法。

【０１０１】＜４＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、ホストテーブルのエントリ新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することに加えて、さらに定期的に各エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することを特徴とする通信ネットワークシステムの管理方法。

【０１０２】＜５＞　前記＜１＞記載の通信ネットワークシステムの管理方法において、ＬＡＮスイッチは、受信パケットの始点ＩＰアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求することに加えて、さらに該パケットの終点ＩＰアドレスに該当するホストテーブルのエントリの新規作成時や書き換えが発生した場合に該エントリのＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求し、始点ＩＰアドレスと同様に終点ＩＰアドレスにつ

いても、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合のみ該エントリの書き換えを行うことを特徴とする通信ネットワークシステムの管理方法。

【０１０３】＜６＞　（ａ）各ポートとの間でパケットの送受信を行う通信処理手段と、（ｂ）前記通信処理手段から渡されたパケットの始点ＭＡＣアドレス、終点ＭＡＣアドレス、始点ＩＰアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＩＰアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、新規作成または書き換えて良いか認証処理手段に問い合わせ、その結果、書き換え禁止の通知を受けた場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、書き換え許可の通知を受けた場合は、終点ＩＰアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートへのパケット出力を前記通信処理手段に指示し、該当エントリが無い場合は、前記ホストテーブルに該当するエントリを新規に作成して、該当ポートへのパケット出力を前記通信処理手段に指示する中継処理手段と、（ｃ）予め管理端末等を介して入力された各ＰＣのＩＰアドレス、ユーザ名、パスワード、連絡先メールアドレス等を登録して認証テーブルを作成し、前記中継処理手段から指示されると、指示されたＩＰアドレスのＰＣにユーザ名とパスワードの入力を要求するメッセージを作成して、前記パケットの受信ポートへの送出を前記通信処理手段に指示するとともに、ユーザ名とパスワードが返されるのを待って、前記認証テーブルの中の前記ＩＰアドレスに該当する連絡先メールアドレスに前記ホストテーブルのエントリ書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記通信処理手段に送出を指示し、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリの書き換え禁止を前記中継処理手段に通知し、予め認証テーブルに登録されているユーザ名とパスワードが得られた場合は、前記ホストテーブルのエントリの書き換え許可を前記中継処理手段に通知する認証処理手段とを具備したことを特徴とするＬＡＮスイッチ。

【０１０４】＜７＞　ＬＡＮスイッチで構成する通信ネットワークシステムの管理方法であって、（ａ）各ＰＣはＬＡＮスイッチに予めＭＡＣアドレスとそのユーザ名、パスワード、連絡先メールアドレスを登録し、（ｂ）ＬＡＮスイッチの管理者も同様にＬＡＮスイッチに予め連絡先メールアドレスを登録し、（ｃ）ＬＡＮスイッチは前記ＰＣおよび前記ＬＡＮスイッチの管理者の情報を登録する認証テーブルを作成し、（ｄ）さらにＬＡＮスイッチは各ＰＣ間の通信のパケットを受信すると、該パケットの始点ＭＡＣアドレスを学習してホストテーブルを作成し、このとき前記ホストテーブルの中に前記始点ＭＡＣアドレスに該当するエントリが無く新規に作成する場合や該当エントリと異なる情報に書き換える場合は、該パケットの受信ポートで且つ該パケットの始点ＭＡＣアドレスのＰＣにユーザ名とパスワードを要求するとともに、ユーザ名とパスワードが返されるのを待って、前記ホストテーブルの書き換え要求が発生した旨を伝えるメッセージを作成し、該メッセージの中にＰＣから返されたユーザ名を情報として入れ、前記認証テーブルの中の前記始点ＭＡＣアドレスに該当する連絡先メールアドレスに送り、さらに予め前記認証テーブルに登録されているユーザ名とパスワードが得られなかった場合や一定時間内に応答が返されなかった場合は、前記ホストテーブルのエントリ書き換えを中止するとともに該パケットを廃棄し、予め前記認証テーブルに登録されているユーザ名とパスワードが得られた場合は、終点ＭＡＣアドレスをキーに前記ホストテーブルを参照し、該当エントリが有る場合は、該当ポートにパケットを出力し、該当エントリが無い場合は、該当するホストテーブルのエントリを新規に作成して、該当ポートにパケットを出力することを特徴とする通信ネットワークシステムの管理方法。

【０１０５】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【０１０６】

【発明の効果】本発明の通信ネットワークシステムの管理方法によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能になる、という効果が得られる。

【０１０７】また、本発明の通信ネットワークシステムの管理方法によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークのセキュリティを向上させることができる、という効果が得られる。

【０１０８】本発明の情報中継装置によれば、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の解析および回復操作の迅速化が可能になる、という効果が得られる。

【０１０９】また、本発明の情報中継装置によれば、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることができる、という効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの構成の一例を示す概念図である。

【図２】本発明の第１の実施形態である通信ネットワー

クシステムの管理方法を実施するＬＡＮスイッチにて用いられるホストテーブルの一例を示す概念図である。

【図３】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチにて用いられる認証テーブルの一例を示す概念図である。

【図４】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

【図５】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

【図６】本発明の第１の実施形態である通信ネットワークシステムの管理方法を実施するＬＡＮスイッチの作用の一例を示すフローチャートである。

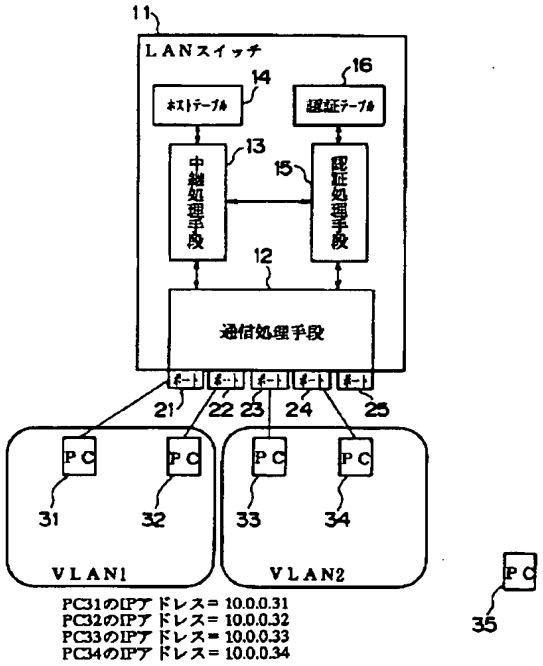
＊【図７】本発明の参考技術であるＩＰサブネットベースＶＬＡＮの一例を示す概念図である。

【符号の説明】

１１…ＬＡＮスイッチ（情報中継装置）、１２…通信処理手段（制御論理）、１３…中継処理手段（制御論理）、１４…ホストテーブル（制御テーブル）、１４ａ…始点ＩＰアドレス、１４ｂ…始点ＭＡＣアドレス、１４ｃ…終点ＭＡＣアドレス、１４ｄ…ポート番号、１４ｅ…帰属ネットワーク、１５…認証処理手段（制御論理）、１６…認証テーブル、１６ａ…ＩＰアドレス、１６ｂ…ユーザ名、１６ｃ…パスワード、１６ｄ…連絡先メールアドレス、２１～２５…ポート（入出力ポート）、３１～３４，３５…ＰＣ、Ａ，Ｂ，Ｃ…メッセージ。

【図１】

図　1



【図２】

図　2

14
ホストテーブル
14a　14b　14c　14d　14e

始点IPアドレス	始点MACアドレス	終点MACアドレス	ポート番号	VLAN
10.0.0.31	10:00:00:00:00:31	10:00:00:00:00:51	21	1
10.0.0.32	10:00:00:00:00:32	10:00:00:00:00:52	22	1
10.0.0.33	10:00:00:00:00:33	10:00:00:00:00:53	23	2
10.0.0.34	10:00:00:00:00:34	10:00:00:00:00:54	24	2

【図３】

図　3

16

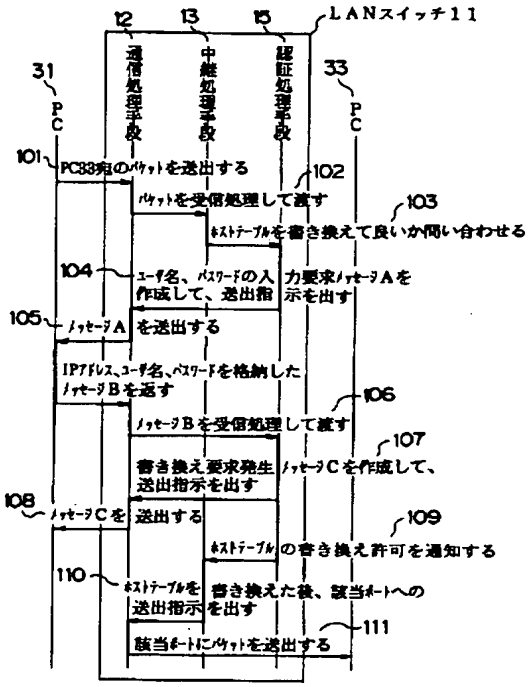
認証テーブル　16b　16c　16d

16a

IPアドレス	ユーザ名	Password	連絡先メールアドレス
10.0.0.31	PC31	pass31	pc31@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.32	PC32	pass32	pc32@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.33	PC33	pass33	pc33@hitachi.co.jp, swlla@hitachi.co.jp
10.0.0.34	PC34	pass34	pc34@hitachi.co.jp, swlla@hitachi.co.jp

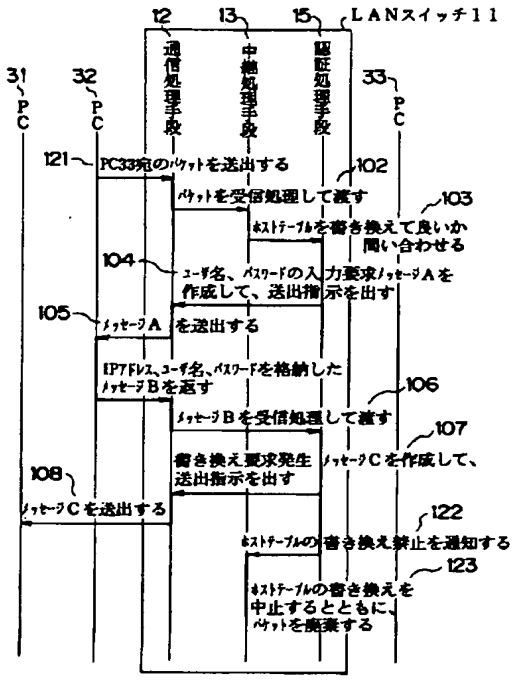
【図４】

図　4



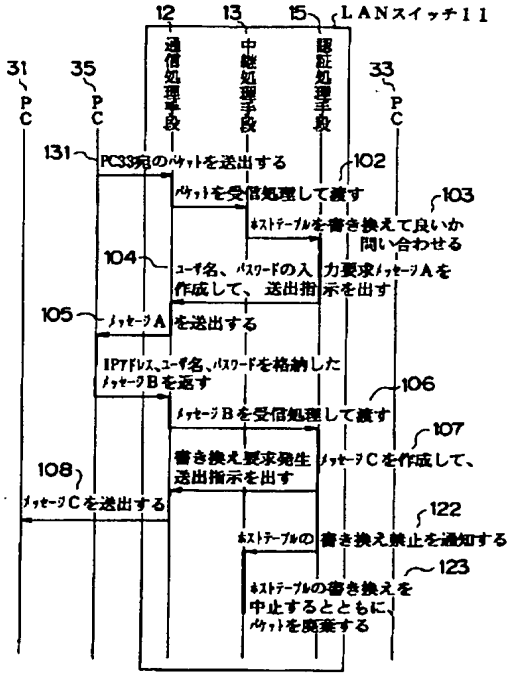
【図５】

図　5



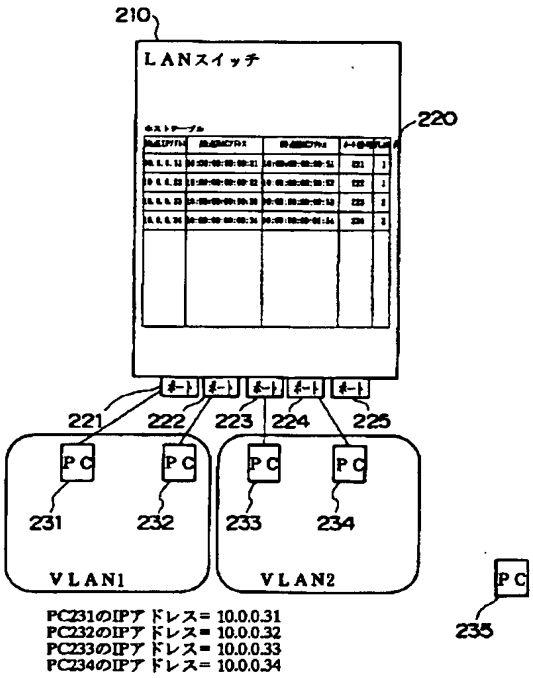
【図６】

図　6



【図７】

図　７



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　29/14			

Ｆターム(参考)　5J104 AA07 KA01 NA05 PA07
5K030 GA11 GA15 GA17 HC14 HD06
HD10 JT09 KA01 KA02 LB05
5K033 AA05 DA05 DB03 DB12 DB14
EC04
5K035 AA06 DD01 LL01
9A001 CC07 CC08 DD10 JJ18 JJ25
KZ56 LL03